Lesson 5. Identity Theft

Lesson Purpose

To focus on methods used to steal an identity and strategies for preventing identity theft.

Learning Objectives

Participants will be able to:

- Recognize common methods used to steal an identity.
- List multiple strategies to reduce the likelihood of identity theft.
- Describe procedures for ordering a credit report and correcting errors.

Materials

Presentation: Identity Theft

Handout(s): Identity Theft Prevention

Supplement: "Identity Theft and Your Social Security Number," from Social

Security Administration. Download at www.ssa.gov/pubs/10064.html

"ID Theft: What's It All About and When Bad Things Happen to

Your Good Name," from the Federal Trade Commission.

Download both at www.consumer.gov/idtheft/

Display copies of checks with Social Security numbers printed on them, or miscellaneous financial documents containing numbers

that could be used for identity theft.

Related Resources

National Crime Prevention Council, www.ncpc.org
Office of the Attorney General of Virginia, www.oag.state.va.us
Federal Trade Commission, Identity Theft Hotline- 877-ID-THEFT,

www.consumer.gov/idtheft

Social Security Administration Fraud Hotline: (800)-269-0271

Lesson Plan

Time	Main Points					
Time Main Points Slide Introduction						
5 min.	The crime of Identity theft is on the rise and has become a significant problem.	1 - 2				
	Briefly describe a recent, local example of identity theft.					
	Today we'll look at some common methods used to steal an identity, strategies for reducing the likelihood of identity theft, and steps to take if you suspect you are a victim of identity theft.					
	Distribute the Handout "Identity Theft."					
	Presentation					
8 min.	Avoid Becoming a Victim of Identity Theft Minimize the information you carry with you. Do not carry extra credit cards, a Social Security card, birth certificate or passport in your wallet or purse, except when needed.	3				
	 To reduce personal information that is in circulation, consider the following: Remove your name from the marketing lists of the three major credit reporting bureaus, i.e., Equifax, Experian (formerly TRW) and Trans Union. Add your name to the computerized name deletion lists used by nationwide marketers. Have your name and address removed from telephone books and reverse directories. Install a locked mailbox at your residence or business to reduce mail theft, or use a post office box. 	3				
	 When you order new checks, do not have them sent to your home address. Have them sent to a post office box or arrange to pick them up at your bank. When you pay bills, do not place the envelopes containing your checks in your home mailbox for the letter carrier to pick up. Pay bills with an electronic bill payment service. Reduce the number of credit cards you actively use to a bare minimum. Carry only one or two credit cards in your wallet. Cancel all unused credit card accounts. Keep a list and/or photocopy of all your credit cards, account numbers, expiration dates and telephone numbers of the customer service and fraud departments in a secure place (not your wallet or purse) so you can quickly contact your creditors in case your credit cards are stolen. Do the same with your bank accounts. 	4				

Time	Main Points	Slide
	 Never provide your credit card number or other personal information over the telephone, unless you have a trusted business relationship with the person or company, and you have initiated the telephone call. Order your credit report once a year from each of the three major credit bureaus to check for inaccuracies and fraudulent use of your accounts. Always take credit card receipts with you. Never throw them in a public trash container. 	4
8 min.	 Watch the mail when you expect a new or reissued credit card to arrive. Contact the issuer if the card does not arrive. When creating a password or Personal Identification Number (PIN), use a number that is not easy for others to determine. Ask your financial institution to add extra security protection to your account. Memorize all your passwords. Do not record them on anything in your wallet or purse. 	5
	 Protect your Social Security number. Release it only when absolutely necessary (tax forms, employment records, most banking, stock and property transactions). The Social Security number is the key to your credit and bank accounts and is a prime target of identity thieves. Do not have your Social Security number printed on your checks. Do not let merchants write your Social Security number on your checks because of the risk of fraud. Order your Social Security Earnings and Benefits Statement once a year to check for fraud. 	6
4 min.	 Carefully review your credit card statements for unauthorized use. Do not throw pre-approved credit offers in the trash or in a recycling container without first shredding them. The discarded credit offers can be used by identity thieves to order credit cards in your name and to have the credit cards mailed to their address. Do the same with other sensitive information like credit card receipts. Home shredders can be purchased at many office supply stores. When you fill out loan applications, find out how the company disposes of them. If you are not convinced that they store them in locked files and/or shred them, take your business elsewhere. Some car dealerships, department stores, car rental agencies and video stores have been known to be careless with customer applications. When you pay by credit card, ask the business how it stores and disposes of the transaction slip. Avoid paying by credit card if you think the business does not use adequate safeguards. Store your cancelled checks in a safe place. In the wrong hands, they can reveal a lot of information about you. Never permit your credit card number to be written on your checks. 	7

Time	Main Points	Slide
8 min.	 If you become a victim of Identity Theft Act immediately to minimize the damage. (See detailed information in handout) When dealing with authorities and financial institutions, keep a log of all conversations, dates, names and telephone numbers. Sometimes victims of identity theft are wrongfully accused of crimes committed by an imposter. You may qualify for a Virginia Identity Theft Passport. 	8
	 Also do the following: (See details in handout) Report the crime to local law enforcement. Immediately contact (by telephone and in writing) all creditors with whom your name has been used fraudulently. If you have had checks stolen or bank accounts set up fraudulently, notify your bank. The U.S. Secret Service has jurisdiction over financial fraud cases, 	9
	but it usually does not investigate individual cases unless the dollar amount is high and/or you are one of many victims of a fraud ring. To interest the Secret Service in your case, you may want to ask the fraud department of the credit card companies and/or banks, as well as the police or sheriff detective/investigator, to notify the particular Secret Service agent they work with regarding your case. Call the Social Security Administration to report fraudulent use of your Social Security number. Call 1-800-269-0271 or download	
	 more information about Social Security numbers and identity theft from http://www.ssa.gov/pubs/idtheft.htm Notify the local Postal Inspector if you suspect an identity thief has filed a change of address with the post office, or has used the mail to commit credit or bank fraud against you. You also may need to talk with your mail carrier. If you have a passport, notify the passport office to be on the 	9
	 lookout for anyone ordering a new passport fraudulently. Call electrical, gas and water utilities. Alert them to the possibility that someone may attempt to open a new service using your identification. You may want to change your driver's license number if someone is using your license as identification to pass bad checks. 	
2 min.	 You may want to consult an attorney to determine legal action to take against creditors and/or credit bureaus if they are not cooperative in removing fraudulent entries from your credit report, or if negligence is a factor. Call the local Bar Association to find an attorney who specializes in consumer law and the Fair Credit Reporting Act. Pay attention to your own mental health. Victims of identity theft often report a sense that they are, themselves, somehow to blame. They often feel violated, even powerless, due to the fact that few, if any, of the authorities they have notified of the crime step forward to help them. 	9

Time	Main Points	Slide
	Do not give-in and do not pay any bill or portion of a bill, which is the result of identity theft. Do not cover any checks which were written and/or cashed fraudulently. Your credit rating should not be permanently affected, and no legal action should be taken against you. If any merchant, financial institution or collection agency suggests otherwise, simply restate your willingness to cooperate, but do not allow yourself to be coerced into paying fraudulent bills.	9
2 min.	 Credit Cards (See details in handout) Immediately call the fraud units of the three credit reporting bureaus: Equifax (800-525-6285), Experian (888-397-3742; formerly TRW) and Trans Union (800-680-7289). Credit Reporting Bureaus Contact credit reporting bureaus for names and telephone numbers of credit grantors with whom fraudulent accounts have been opened. The nearest office of the Consumer Credit Counseling Service might be able to give you advice about how to remove fraudulent claims from your credit report. Report the theft of your credit cards or numbers. Ask that your accounts be flagged. Also, add a victim's statement to your report, up to 100 words. ["My Identification has been used to apply for credit fraudulently. Contact me at (telephone number) to verify all applications."] Be sure to ask how long the fraud alert is posted on your account, and ask how you can extend it if necessary. Be aware that these measures may not entirely stop new fraudulent accounts from being opened by an imposter. Ask the credit bureaus, in writing, to provide you with free copies every few months, so you can monitor your credit report. 	10
2 min.	 Summarizing Protect your private information and monitor accounts for signs of identity theft. If you are a victim, act quickly to correct the situation with a broad range of agencies and organizations. Practice/feedback	11
10 min.	Have participants review the list of tips for preventing identity fraud in	12
10 111111.	their handout. Ask them to place a checkmark (√) beside the things they now do and to place an asterisk (*) beside the things that they need to begin to do. Give participants 5 to 7 minutes to complete this review. The instructor should circulate among participants during this time. Conclude the activity by asking a couple of volunteer participants to share what they learned from the review. The instructor should reinforce prevention strategies and key learning points.	12

Time	Main Points	Slide	
Evaluation			
10 min.	Set-up We have a few minutes for questions and additional discussion. While we're doing that, we have a brief evaluation form we'd like for you to complete and leave with us. Your name is not required, but your	13	
	feedback is very important. It will help us improve our presentation and program.		
	Distribute evaluation forms and ask for questions or additional comments on what has been presented.		
	Promote group discussion by encouraging audience members to help respond to questions. Use questions as an opportunity to clarify and reinforce key learning objectives.		
	Wrap-up		
	 Thank the audience for their attention and participation. Express appreciation to the sponsoring organization for the opportunity to speak. 		
	 Remind them to leave evaluation forms. 		

5. Identity Theft

Please tell us what you think about this lesson by circling the numbers that most closely reflect your opinions.

After this lesson	Strongly Disagree	Disagree	Agree	Strongly Agree
a) I am better able to recognize common methods to steal an identity.	1	2	3	4
b) I know more strategies to reduce the likelihood of identity theft.	1	2	3	4
c) I know more about how to monitor my credit record and to correct errors detected.	1	2	3	4
d) I am now more likely to report activities or inquiries that seek personal information that could be used for identity theft.		2	3	4
About this lesson	28	PR		
e) The information presented was valuable.	1	2	3	4
f) The lesson was presented in a clear and understandable manner.	1	2	3	4
g) Lesson activities and discussion were helpful.	1	2	3	4
h) I would recommend this lesson to others.	1	2	3	4

What was the most valuable thing you learned?

Please give one example of how you plan to use the information presented in this lesson.

How could this lesson be improved?